Untitled document

By Congressman Charles F. Bass
Published on NH Patch websites, February 23, 2012

The global threat of cyber attack, once relegated to the silver screen, is posing an ever-increasing challenge to New Hampshire individuals and businesses. In fact, two years ago, one local company learned just how real, and how devastating, being victimized by cybercrime can be.

In 2010, a Hudson, New Hampshire-based IT consultant was contacted by its bank to discuss an automated clearinghouse fund transfer. Upon returning the call, the owner learned that his company had been fleeced for nearly $100,000 in unauthorized transactions. An unknown person had authorized payment to 10 individuals that had been surreptitiously added to the company's payroll, sending each one just under $10,000. When the company followed up with the bank, they learned that the money was uninsured and they would be unable to recoup the loss.

The company wasn't the victim of an armed robbery, but the victim of the Zeus Trojan. This malicious software, or malware, records keystrokes made on an infected computer, giving a hacker access to every password and file stored on the victim's hard drive. What makes the Zeus Trojan so dangerous is that it is often times undetectable, even by the most up-to-date antivirus programs. With antivirus software showing a limited effect, and small and medium businesses being viciously targeted, the question currently being posed by Congress is what can be done to protect our companies, and our economy, from cyber attacks?

I recently took part in a Committee on Energy and Commerce Subcommittee on Communications and Technology hearing on cybersecurity. Testimony from five of the foremost experts in cyber defense provided interesting insight into the goals of the hacking community, the breadth and depth of the risk to American businesses, and most importantly, outlined several strategies for how the American small business community can adapt in order to overcome specific threats.

From witness testimony, I learned about the evolving goals of the online hacking community. While these groups were once content to hack in order to cause mischief and earn online bragging rights, the game has changed to hacking for harm and profit. This has raised the costs of cybersecurity as the risk of network insecurity is devastating.

What is also evident is that this crisis will not be solved by static laws and outdated regulations that cannot adapt to the constant changes of cyber criminals, many of whom operate outside the United States. We must be smarter, more agile, and have the tools in place to prevent and prosecute the criminals lurking on the Internet.

Cyber threats are a very real threat to the stability and security of our economy and way of life. Protecting New Hampshire individuals and businesses from cyber attacks will take diligence, both from companies and from the government. America needs a coordinated plan of action,

where government agencies work with private cybersecurity firms in order to mitigate the effects of cybercrime and companies are educated on the best defenses.

Although the solutions may not be obvious or immediate, as a member of Energy and Commerce, I am committed to finding them by working with industry and all stakeholders to protect America from this advancing threat.

-- 30 --

Congressman Charles F. Bass represents New Hampshire's Second District in Congress. You can contact him at http://bass.house.gov.